UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,209	02/03/2006	Wilhelmus Franciscus Johanne Verhaegh	NL031006	9671

24737 7590 11/19/2007

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	PAPER NUMBER
4172	
MAIL DATE	DELIVERY MODE
11/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/567,209	VERHAEGH ET AL.	
	Examiner	Art Unit	
	Christopher C. Johns	4172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/23/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Drawings

New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings do not accurately reflect the inventive object or limitations. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 112

Claim 2 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is not clear how the "encrypted inner product" is calculated.

Claim Rejections 35 U.S.C. 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 13 rejected under 35 U.S.C. 101 because it is drawn to functional descriptive material that is not embodied on a computer-readable medium. See MPEP §2106.01.

Claim 13 rejected under 35 U.S.C. 101 because it is drawn to a computer program product, dependent from an independent claim that is drawn to the system in claim 1. This claim covers two statutory classes of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3, 4 and 6-13 rejected under 35 U.S.C. 102(b) as being anticipated by "Collaborative Filtering with Privacy", a paper by John Canny in the Proceedings of the 2002 IEEE Symposium on Security and Privacy (hereafter referred to as Canny).

As per claim 1:

Canny covers:

- a first source for encrypting first data and a second source for encrypting second data (cf. section 3.2, where the clients are said to have "data values..." and "To encrypt, user chooses random values…", encrypting them by using "a standard El-Gamal encryption of the exponentiation of a vote"),

- a server configured to obtain the encrypted first and second data (cf. Abstract, where the system is said to be a "server-based collaborative filtering system"),
- the server being precluded from decrypting the encrypted first and second data and from revealing identities of the first and second sources to each other (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data."),
- computation means for performing a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community, or by outsiders", and section 2.1 "Given a vector of user preferences *P*, the most likely pair (*x*, *n*) is the pair that minimizes $x^2/(2\sigma_x^2) + n^2/(2\sigma_n^2)$").

As per claim 4:

Canny discloses:

- computation means to obtain an encrypted inner product between the first data and the second data, or encrypted sums of shares of the first and second data in

the similarity value (cf. section 1.2, where another paper is mentioned that "used simple inner products to generate recommendations"),

- that the server is coupled to a public-key decryption server for decrypting the encrypted inner product or the sums of shares and obtaining the similarity value (cf. section 3.2, where the values are said to be "a standard El-Gamal encryption", which is a public-key cryptosystem).

As per claim 5:

Canny discloses that the:

- similarity value can be obtained using a Pearson correlation (cf. section 5.3, 2nd paragraph, "For instance, Pearson correlation and personality diagnosis use the entire user dataset to generate new recommendations").

As per claim 6:

Canny discloses:

- encrypting first data for a first source, and encrypt second data for a second source (cf. section 3.2, where the clients are said to have "data values..." and "To encrypt, user chooses random values…", encrypting them by using "a standard El-Gamal encryption of the exponentiation of a vote"),
- providing the encrypted first and second data to a server that is precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data."),

- performing a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community, or by outsiders", and section 2.1 "Given a vector of user preferences P, the most likely pair (x, n) is the pair that minimizes $x^2/(2\sigma_x^2) + n^2/(2\sigma_n^2)$").

As per claim 7:

Canny discloses:

- that the first or second data comprises a user profile of a first or second user respectively, the user profile indicating user preferences of the first or second user to media content items (cf. Abstract, where it is said that these sort of systems are useful in "e-commerce and…direct recommendation applications"; and section 1, where it is said that using collaborative filtering systems is well known in areas such as "personalized purchase recommendations", and that users could obtain recommendations about "restaurants, bars, movies, and interesting sights…").

As per claim 8:

Canny discloses:

- that comprises user ratings of respective content items (cf. Abstract, where it is said that these sort of systems are useful in "e-commerce and…direct recommendation applications"; and section 1, where it is said that using collaborative filtering systems is well known in areas such as "personalized purchase recommendations", and that users could obtain recommendations about "restaurants, bars, movies, and interesting sights…").

As per claim 9:

Canny discloses:

- using the similarity value to obtain a recommendation of a content item for the first or second source (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community, or by outsiders", and section 2.1 "Given a vector of user preferences *P*, the most likely pair (*x*, *n*) is the pair that minimizes $x^2/(2\sigma_x^2) + n^2/(2\sigma_n^2)$").

As per claim 10:

Canny discloses:

- that the recommendation is performed using a collaborative filtering technique (cf. Abstract, first sentence).

As per claim 11:

Canny discloses:

- a server being configured to obtain encrypted first data of a first source and encrypted second data of a second source (cf. Abstract, where the system is said to be a "server-based collaborative filtering system"; and section 3.2, where the clients are said to have "data values..." and "To encrypt, user chooses random values…", encrypting them by using "a standard El-Gamal encryption of the exponentiation of a vote"),
- the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data."),
- enabling a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community, or by outsiders", and section 2.1 "Given a vector of user preferences *P*, the most likely pair (*x*, *n*) is the pair that minimizes $x^2/(2\sigma_x^2) + n^2/(2\sigma_n^2)$").

As per claim 12:

Canny discloses:

- obtaining encrypted first data of a first source and encrypted second data of a second source by a server (cf. Abstract, where the system is said to be a "server-based collaborative filtering system"; and section 3.2, where the clients are said to have "data values..." and "To encrypt, user chooses random values…", encrypting them by using "a standard El-Gamal encryption of the exponentiation of a vote"),
- the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data."),

enabling a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data (cf. Abstract – "We describe an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community, or by outsiders", and section 2.1 "Given a vector of user preferences P, the most likely pair (x, n) is the pair that minimizes $x^2/(2\sigma_x^2) + n^2/(2\sigma_n^2)$").

As per claim 13:

Claim 13 is a computer program that embodies the exact same limitations in claim 1, and is similarly rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2 and 3 rejected under 35 U.S.C. 103(a) as being unpatentable over Canny, in view of the Paillier cryptosystem.

As per claim 2:

Canny discloses:

- obtaining an encrypted inner product between the first data and the second data (cf. section 1.2; while Canny's system does not accomplish these means, it is mentioned that another similar system "used simple inner products to generate recommendations", and it would be obvious to one skilled in the art at the time of the invention to encrypt the inner products, in order to protect data),
- providing the encrypted inner product to the first source via the server, the first source being configured to decrypt the encrypted inner product for obtaining the

similarity value (cf. section 1.2, where if the data were encrypted in the referenced system, it would need to be decrypted in order to be understood).

As per claim 3:

Canny discloses:

- the computation means is realized using a Paillier cryptosystem, or a threshold Paillier cryptosystem using a public key-sharing scheme (cf. Appendix A, page 12, where the system uses "cryptographic homomorphism" for the computation of the vector sums. It does not explicitly mention using a Paillier cryptosystem or a threshold Paillier cryptosystem for the computation. The Paillier cryptosystem, published in EUROCRYPT in 1999, is a homomorphic public-key cryptosystem that is based on composite degree residuosity classes. In the original paper, on page 236, Paillier notes that the system is useful for self-blinding data, and, on page 235, that it possesses additive homomorphic properties (meaning that data can be added to encrypted data without needing to decrypt the original data). The system in Canny does not explicitly use the Paillier cryptosystem for its computations. However, the Paillier system is a cryptosystem that would do exactly what the system in Canny desires – it is a homomorphic cryptosystem that allows for self-blinding. The motivation to use the Paillier system exists because it is perfectly suited for Canny's needs, and would be a simple substitution for Pedersen's scheme (cf. section 3.1, "After applying Pedersen's protocol…"). Therefore, it would have been obvious to one skilled in the art at the time of

the invention to use the Paillier cryptosystem in the system in Canny, because of the interchangeability and the motivating statements in the Paillier publication.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is 571-270-3462. The examiner can normally be reached on Monday-Thursday, 7:30-5, Alternate Fridays, 7:30-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tom Dixon can be reached on 571-272-6803. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher C Johns/
Examiner, Art Unit 4172

Christopher Johns
Examiner
Art Unit 4172

CCJ

/Naeem Haq/
Primary Examiner, Art Unit 4172